[Insert Company Name and Logo]	
Title: Use of Mobile Devices	**P&P #:**
Approval Date:	**Review: Annual**
Effective Date:	**Security Team**

Purpose: This policy governs the authorized use of smartphones and other portable computing and communications devices by authorized members of workforce.

Scope: This policy applies to all electronic computing and communications devices which may be readily carried by an individual and is capable of storing, receiving, processing, or transmitting digital information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other portable device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices).

This Policy also applies to personally-owned Mobile Devices (best practice is to require that personal devices not be used at all) as well as mobile devices owned or leased and provided by [Insert Company name].

Prohibited Mobile Devices:

> Mobile devices which may produce electromagnetic interference with medical devices or equipment, or which cannot be or have not been configured to comply with this Policy, are prohibited.

Definitions:

1. User: Any employee or other workforce member (whether paid or volunteer) authorized by [Insert Company name] to read, enter or update information created or transmitted via an electronic system.
2. Mobile Devices: Includes, but is not limited to smartphones, portable hard drives and USB (thumb) drives, digital music players, hand-held computers, laptop computers, tablet computers, and personal digital assistants (PDAs).

Policy: Mobile devices can be used to provide more efficient workflow and administrative processes within organizations. At the same time, the use of such devices creates new risks to secure sensitive and regulated data, as well as data and organizational confidentiality, and intellectual property. This Policy is intended to permit the use of such devices while managing the risks they present.

Procedure:

In order to maintain the confidentiality and integrity of the mobile devices, [Insert Company name] will (choose from the following what best fits your organization):

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

1. Keep an inventory of all mobile devices used by workforce to access and transmit data.
2. Store mobile devices, when not in use, in locked offices or lockers.
3. Install radio frequency identification ("RFID") tags on mobile devices to help locate a lost or stolen mobile device.
4. Use remote shutdown tools to prevent data breaches by remotely locking mobile devices.
5. Install and regularly update anti-malicious software (also called malware) on mobile devices.
6. Install firewalls where appropriate.
7. Apply encryption to all sensitive and regulated data.
8. Install IT backup capabilities, such as off-site data centers and/or private clouds, to provide redundancy and continued access to data.
9. Adopt biometric authentication tools to verify the user is authorized to access the sensitive and regulated data.
10. Ensure mobile devices use is secure, encrypted Hypertext Transfer Protocol Secure ("HTTP") similar to those used in banking and financial transactions to provide encrypted communication and secure identification of a network web server.
11. Use of portable devices shall employ approved VPN technology when establishing communication links.
12. Mobile devices accessing wireless networks must meet the following criteria:
    i. Mobile devices must use encryption for secure information transfers.
    ii. Portable devices using only WEP encryption technology will not be approved for the transfer of sensitive and regulated data.
    iii. Portable devices using publicly accessible wireless infrastructures and accessing sensitive and regulated data shall employ two-factor authentication as defined in accordance with [Insert Company name] practices.
13. System Administrators shall ensure that sensitive and regulated data subject to final disposition is disposed of by using a method that ensures the data cannot be recovered or reconstructed.
    i. The Security Officer shall maintain documentation of such data destruction that lists the device, the date of destruction, the workforce personnel authorizing the destruction, general description of the sensitive or regulated data (if available), and the identity of the workforce personnel performing the destruction.

2. Authorization to Use Mobile Devices.
    1. No Mobile Device may be used for any purpose or activity involving information subject to this Policy without prior registration of the device and written authorization by [Insert Company name]. Authorization will be given only for use

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

of Mobile Devices which [Insert Company name] has confirmed and configured to comply with this Policy. Authorization must be requested in writing by the department manager.

2. Access to, obtaining, use and disclosure of information subject to this Policy by a mobile device, and any use of a mobile device in any [Insert Company name] facility or office, including an authorized home office or remote site, must follow all [Insert Company name] policies at all times.

3. Authorization to use a Mobile Device may be suspended at any time:
    1. If the User fails or refuses to comply with this Policy.
    2. In order to avoid, prevent or mitigate the consequences of a violation of this Policy.
    3. In connection with the investigation of a possible or proven security breach, security incident, or violation of [Insert Company name] policies.
    4. In order to protect individual life, health, privacy, reputational and/or financial interests.
    5. To protect any assets, information, reputational or financial interests of [Insert Company name].
    6. Upon request of the department manager, with justification from above list.
4. Authorization to use a Mobile Device terminates:
    1. Automatically upon the termination of a User's status as a member of the [Insert Company name] workforce.
    2. Upon a change in the User's role as a member of the [Insert Company name] workforce, unless continued authorization is requested by the department manager.
    3. If it is determined that the User violated this or any other [Insert Company name] policy.
    4. The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.
5. Audit of Mobile Devices:
    1. Any mobile device may be subject to audit to ensure compliance with this and other [Insert Company name] policies. This includes personally owned mobile devices (you can require that personal devices not be used at all) as well as mobile devices owned or leased and provided by [Insert Company name].
        i. Any User receiving such a request shall transfer possession of the mobile device to the IT Department at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the mobile device after receiving the request.
6. Evidentiary Access to Mobile Devices:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

1. Upon notice of a litigation hold by the IT Department or Legal Department, at their sole discretion at any time, any mobile device may be subject to transfer to the possession of the IT Department to ensure compliance with the litigation hold. Any User receiving such a notification shall transfer possession of the mobile device to the IT Department at once, unless a later transfer date and time is indicated in the notification, and shall not delete or modify any information subject to this Policy, which is stored on the mobile device after receiving the request.

7. Mobile Device User Responsibilities:
    1. In addition to other requirements and prohibitions of this and other [Insert Company name] policies, mobile device users have the following responsibilities:
        i. Information subject to this Policy, which is stored on the mobile device, must be encrypted as provided in [Insert Company name] policy. Information subject to this Policy should not be stored on the mobile device for any period longer than necessary for the purpose for which it is stored.
        ii. A mobile device may not be shared at any time when unencrypted information subject to this Policy is stored on the device.
        iii. A mobile device which does not have unencrypted information subject to this Policy stored on it may be shared temporarily, provided that:
            1. The User may not share the password or PIN used to access the mobile device. The User may input the password or PIN for an alternate user in the event shared use is required.
            2. The configuration of the device, to comply with this Policy, must not be changed.
            3. The individual using the device, not the authorized user, must not further share it; must protect it against being misplaced, lost or stolen, and must immediately report to the User if it is; and must return it promptly to the authorized user when finished with the temporary use.
            4. The individual using the device must not use it to obtain, process, use or disclose information subject to this Policy.
        iv. Access to each mobile device must be controlled by a password or PIN number consistent with [Insert Company name] policy. Password or PINs must be changed periodically as provided in [Insert Company name] policy. The mobile device must provide for a maximum of 3 attempts to enter the password or PIN correctly.
        v. The timeout for access to the mobile devices must be a maximum of 15 minutes.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

vi. Information subject to this Policy which is transmitted wirelessly by the mobile device must be encrypted unless an exception is authorized. Exceptions must be authorized by the IT Department.
vii. If possible, mobile devices must have antivirus software. Mobile devices that cannot support antivirus software may be subject to limitations on use at the discretion of the IT Department as specified in writing by the IT Department.
viii. Physical protection for mobile devices must be provided as required by [Insert Company name] policy.
ix. Mobile devices shall not be left unattended in public areas.
x. If the mobile device is misplaced, stolen or believed to be compromised this must be immediately reported to the Security Officer.
xi. Applications and services installed on the mobile device must be approved by the IT Department.
xii. Bluetooth and infrared (IR) services must be configured as approved by the IT Department or turned off.
xiii. Mobile devices must be disposed of according to [Insert Company name] policy.

8. Personal Use of Mobile Devices.
    1. Personal use of mobile devices owned or leased and provided by [Insert Company name] is subject to the [Insert Company name] Acceptable Use Policy.
    2. Personal use of personally owned mobile devices is not subject to the Acceptable Use Policy, but must at all times be consistent with this Policy.
    3. All information on a mobile device, including personal information about or entered by the User, may be subject to audit or evidentiary review as provided in this Policy. Any such personal information may be used or disclosed by [Insert Company name] to the extent it deems reasonably necessary:
        i. In order to avoid, prevent or mitigate the consequences of a violation of this Policy.
        ii. In connection with the investigation of a possible or proven security breach, security incident, or violation of [Insert Company name] policies.
        iii. In order to protect the life, health, privacy, reputational or financial interests of any individual.
        iv. To protect any assets, information, reputational or financial interests of [Insert Company name].
        v. For purposes of determining sanctions against the User or any other member of the [Insert Company name] workforce.
        vi. For purposes of litigation involving the User.
        vii. If Required by Law.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

9. Prohibited Uses of Mobile Devices.
    1. The following uses of mobile devices are prohibited:
        i. The storage of information subject to this Policy, including voice messages, photographs, voice notes, email, instant messages, web pages and electronic documents, images and videos, unless they are encrypted.
        ii. The Internet, wireless transmission or upload of information subject to this Policy, including voice messages, photographs, voice notes, email, instant messages, web pages and electronic documents, images and videos, without encryption, unless previously authorized in writing by the IT Department.
        iii. The creation of any photograph, image, video, voice or other recording of any individual who is a patient or member of the Workforce of [Insert Company name], except in compliance with [Insert Company name] policy.
        iv. The creation of any photograph, image, video, voice or other recording of any document, record, computer or device screen that includes information subject to this Policy, except in compliance with [Insert Company name] policy.

Violations:
Any known violations of this policy should be reported to the Security Officer. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action, up to and including termination. [Insert Company name] may advise law enforcement agencies when a criminal offense may have been committed.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.